

Rabin Verschlüsselung 1979

Idee: Rabin Verschlüsselung

- Beobachtung: Berechnen von Wurzeln in \mathbb{Z}_p ist effizient möglich.
- Ziehen von Quadratwurzeln in \mathbb{Z}_N ist äquivalent zum Faktorisieren.

Vorteil: CPA-Sicherheit beruht nur auf Faktorisierungsannahme.

Für unsere bisherigen Verfahren verwendeten wir *stärkere* Annahmen.

- RSA: Berechnen von e -ten Wurzeln in \mathbb{Z}_n .
- Goldwasser-Micali: Unterscheiden von QR_N und QNR_N^{+1} .

Berechnen von Quadratwurzeln in \mathbb{Z}_p

Satz Ziehen von Wurzeln in \mathbb{Z}_p

Sei p prim mit $p = 3 \pmod 4$ und $a \in QR_p$. Dann gilt für $b^2 = a \pmod p$, dass $b = \pm a^{\frac{p+1}{4}} \pmod p$. Ferner ist $a^{\frac{p+1}{4}} \in QR_p$ und $-a^{\frac{p+1}{4}} \in QNR_p$

Beweis:

- Es gilt $(\pm a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a = \left(\frac{a}{p}\right) \cdot a = a \pmod p$.

- Wir schreiben $p = 4k + 3$. Dann gilt

$$\left(\frac{-a^{\frac{p+1}{4}}}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a^{\frac{p+1}{4}}}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{a}{p}\right)^{\frac{p+1}{4}} = (-1)^{2k+1} = (-1).$$

- Damit folgt $-a^{\frac{p+1}{4}} \in QNR_p$ und $a^{\frac{p+1}{4}} \in QR_p$.

Quadratwurzel bei bekannter Faktorisierung

Definition Blum-Zahl

Sei $N = pq$ ein RSA-Modul. N heißt *Blum-Zahl* falls $p = q = 3 \pmod{4}$.

Satz Quadratwurzeln in \mathbb{Z}_N

Sei $N = pq$ eine Blum-Zahl mit bekannten p, q . Dann können die vier Quadratwurzeln von $a \in QR_N$ in Zeit $\mathcal{O}(\log^3 N)$ berechnet werden.

Beweis:

Algorithmus QUADRATWURZEL

EINGABE: $N, p, q, a \in QR_N$

① Berechne $x_p \leftarrow a^{\frac{p+1}{4}} \pmod{p}$, $x_q \leftarrow a^{\frac{q+1}{4}} \pmod{q}$.

② Berechne mittels Chinesischem Restsatz die Lösungen von

$$\left| \begin{array}{l} b_1 = x_p \pmod{p} \\ b_1 = x_q \pmod{q} \end{array} \right|, \left| \begin{array}{l} b_2 = -x_p \pmod{p} \\ b_2 = x_q \pmod{q} \end{array} \right|, \left| \begin{array}{l} b_3 = x_p \pmod{p} \\ b_3 = -x_q \pmod{q} \end{array} \right|, \left| \begin{array}{l} b_4 = -x_p \pmod{p} \\ b_4 = -x_q \pmod{q} \end{array} \right|$$

AUSGABE: b_1, \dots, b_4 mit $b_i^2 = a \pmod{N}$

Satz Existenz einer Hauptwurzel

Sei $N = pq$ eine Blumzahl. Dann besitzt jedes $a \in QR_N$ genau ein $b \in QR_N$ mit $b^2 = a \pmod N$. Wir bezeichnen b als *Hauptwurzel*.

Beweis:

- Algorithmus QUADRATWURZEL liefert

$$b_1 \simeq (x_p, x_q) \in QR_p \times QR_q.$$

- Damit ist $b_1 \in QR_N$ eine Hauptwurzel.
- Alle anderen Wurzel b_2, b_3, b_4 sind keine Hauptwurzeln.
- Z.B. gilt $b_2 = (-x_p, x_q) \in QNR_p \times QR_q$ und damit $b_2 \in QNR_N$.

Quadratwurzeln ohne Faktorisierung

Spiel Wurzelziehen $SQR_{\mathcal{A}, GenModulus}(n)$

1 $(N, p, q) \leftarrow GenModulus(1^n)$

2 Wähle $z \in_R QR_N$.

3 $y \leftarrow \mathcal{A}(1^n, N, z)$

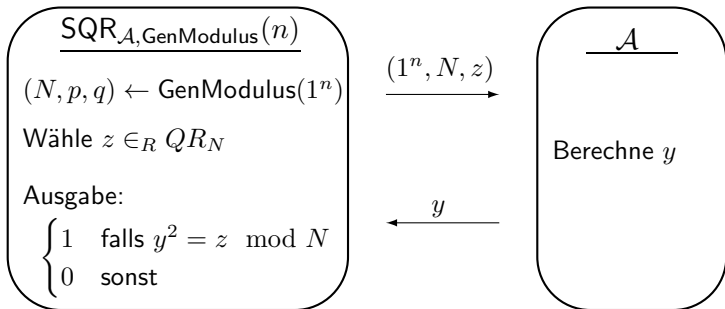
4 $SQR_{\mathcal{A}, GenModulus}(n) = \begin{cases} 1 & \text{falls } y^2 = z \pmod N \\ 0 & \text{sonst} \end{cases}$.

Definition Quadratwzelannahme

Das Berechnen von Quadratwurzeln ist hart bezüglich $GenModulus$, falls für alle ppt \mathcal{A} gilt $Ws[SRQ_{\mathcal{A}, GenModulus}(n) = 1] \leq \text{negl}(n)$.

Quadratwzelannahme: Berechnen von Quadratwurzeln ist hart.

Spiel Wurzelziehen



Nicht-triviale Quadratwurzeln

Satz Faktorisieren mit Wurzeln

Sei $N = pq$ ein RSA-Modul. Seien $x, y \in \mathbb{Z}_N^*$ mit $x^2 = y^2 \pmod N$ und $x \not\equiv \pm y \pmod N$. Dann können p, q in Zeit $\mathcal{O}(\log^2 N)$ berechnet werden.

Beweis:

- Mittels CRT erhalten wir $x \simeq (x_p, x_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.
- Es gilt $y \simeq (x_p, -x_q)$ oder $y \simeq (-x_p, x_q)$.
- Wir betrachten den Fall $y \simeq (x_p, -x_q)$. Der zweite Fall ist analog.
- Es gilt $x + y \simeq (2x_p, 0)$ bzw. $x - y \simeq (0, 2x_q)$.
- Damit folgt $\text{ggT}(N, x + y) = q$ bzw. $\text{ggT}(N, x - y) = p$ wegen $2x_p \in \mathbb{Z}_p^*$ und $2x_q \in \mathbb{Z}_q^*$.
- Die ggT-Berechnung benötigt Laufzeit $\mathcal{O}(\log^2 N)$.

Quadratwurzeln implizieren Faktorisierung

Satz Quadratwurzeln implizieren Faktorisierung

Quadratwurzel- und Faktorisierungsannahme sind äquivalent.

Beweis:

- Bereits gezeigt: Faktorisierung impliziert Quadratwurzeln.
- Sei \mathcal{A} Angreifer im Spiel $SQR_{\mathcal{A}, GenModulus}(n)$ mit Erfolgsws $\epsilon(n)$.
- Konstruieren einen Angreifer \mathcal{A}' im Spiel $Factor_{\mathcal{A}', GenModulus}(n)$.

Algorithmus \mathcal{A}'

EINGABE: N

- 1 Wähle $x \in \mathbb{Z}_N^*$ und berechne $z \leftarrow x^2 \bmod N$.
- 2 $y \leftarrow \mathcal{A}(1^n, N, z)$
- 3 Falls $x = \pm y \bmod N$ oder $x^2 \neq y^2 \bmod N$, Abbruch.

AUSGABE: $p, q = \{\text{ggT}(N, x + y), \text{ggT}(N, x - y)\}$

Faktorisieren mit Quadratwurzeln

- Unter der Faktorisierungsannahme gilt

$$\begin{aligned} \text{negl}(n) &\geq \text{Ws}[\text{Factor}_{\mathcal{A}', \text{GenModulus}}(n) = 1] \\ &= \text{Ws}[x \neq \pm y \bmod N \wedge x^2 = y^2 \bmod N] \\ &= \text{Ws}[x \neq \pm y \bmod N \mid x^2 = y^2 \bmod N] \cdot \text{Ws}[x^2 = y^2 \bmod N] \\ &= \text{Ws}[x \neq \pm y \bmod N \mid x^2 = y^2 \bmod N] \cdot \epsilon(n) \\ &= \frac{1}{2} \cdot \epsilon(n) \end{aligned}$$

- Die letzte Gleichung folgt, da x^2 exakt vier Wurzeln in \mathbb{Z}_N^* besitzt.

Einwegfunktion unter Quadratwurzelannahme

Definition Einwegfunktion QUADRAT

Definieren *Einwegfunktionenfamilie* QUADRAT = (Gen, Samp, f) als

- 1 **Gen**(1^n) : $(N, p, q) \leftarrow \text{GenModulus}(1^n)$, Ausgabe $I = N$.
Definiert $f : \mathbb{Z}_N^* \rightarrow QR_N$.
- 2 **Samp**(I) : Wähle $x \in_R \mathbb{Z}_N^*$ zufällig.
- 3 **$f_I(x)$** : Berechne $f(x) := x^2 \pmod N$.

Anmerkungen:

- QUADRAT ist Einwegfunktion unter der Quadratwurzelannahme.
- D.h. QUADRAT ist Einwegfunktion unter Faktorisierungsannahme.
- **Ziel:** Konstruktion einer Trapdoor-Einwegpermutation.

RABIN Trapdoor-Einwegpermutation

Definition RABIN Trapdoor-Einwegpermutation

Trapdoor-Einwegpermutationsfamilie $RABIN = (Gen, Samp, f)$ mit

- 1 **Gen**(1^n) : $(N, p, q) \leftarrow GenModulus(1^n)$ mit Blumzahl N .
Ausgabe $I = N$, $td = (p, q)$. Definiert $f : QR_N \rightarrow QR_N$.
- 2 **Samp**(I) : Wähle $r \in_R \mathbb{Z}_N^*$ zufällig. Berechne $x \leftarrow r^2 \bmod N$.
- 3 $f_I(x)$: Berechne $y = f(x) := x^2 \bmod N$.
- 4 $Inv_{td}(y)$: Bestimme Hauptwurzel $x \in QR_N$ von $y = x^2$.

Anmerkungen:

- RABIN ist einweg unter der Faktorisierungsannahme. Wir wissen:
Trapdoor-Einwegpermutation + Hardcore-Prädikat
= CPA-sichere Verschlüsselung.
- Benötigen ein Hardcore-Prädikat $hc : QR_N \rightarrow \{0, 1\}$ für f .

Berechnen des niederwertigsten Bits

Satz Hardcore-Prädikat $lsb(x)$

Sei f die RABIN Trapdoor-Einwegpermutation und N eine Blumzahl. Für $x \in QR_N$ bezeichne $lsb(x)$ das niederwertigste Bit von x . Dann ist $hc(x) := lsb(x)$ ein Hardcore-Prädikat für f .

- ohne Beweis (nicht-trivial)
- Für alle ppt \mathcal{A} gilt damit $W_s[\mathcal{A}(1^n, N, x^2) = lsb(x)] \leq \frac{1}{2} + \text{negl}(n)$.

RABIN Kryptosystem (1979)

Algorithmus RABIN Verschlüsselung

- 1 **Gen:** $(N, p, q) \leftarrow \text{GenModulus}(1^n)$, wobei N eine Blumzahl ist.
Ausgabe $pk = N$, $sk = (p, q)$.
- 2 **Enc:** Für $m \in \{0, 1\}$ wähle $r \in \mathbb{Z}_N^*$, berechne $x \leftarrow r^2 \bmod N$ und
 $c \leftarrow (x^2 \bmod N, \text{lsb}(x) \oplus m)$.
- 3 **Dec:** Für $c = (c_1, c_2)$ berechne Hauptwurzel x von c_1 und
 $m := \text{lsb}(x) \oplus c_2$.

Satz CPA-Sicherheit von RABIN

RABIN Verschlüsselung ist CPA-sicher unter der Faktorisierungsannahme.

Beweis:

- Folgt aus dem Satz zur CPA-Sicherheit von $\text{VERSCHLÜSSELUNG}_{\Pi}$.

Diskussion RSA versus RABIN

Vergleich: RSA und RABIN

- Quadrieren und Exponentieren mit e erscheinen ähnlich.
- Aber: RABIN ist kein Spezialfall von RSA, da $e = 2 \notin \mathbb{Z}_{\phi(N)}^*$.
- RABIN-Einwegpermutation beruht auf Faktorisierungsannahme.
- Die Faktorisierungsannahme ist möglicherweise schwächer als die RSA-Annahme. Offen: Invertieren von RSA \Rightarrow Faktorisierung?
- RABIN ist nicht ineffizienter als RSA.

- Historische Variante: Textbook RABIN mit $c := m^2 \bmod N$.
- Es existiert ein CCA-Angriff auf Textbook RABIN, der p, q liefert. (Wie?)